CVE-2009-0126

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2009-0126
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-01-15 17:30:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	The decrypt_public function in lib/crypt.cpp in the client in Berkeley Open Infrastructure for Network Computing (BOINC) 6.2

Risk And Classification

Primary CVSS: v2.0 5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:N/A:N

Problem Types: CWE-287 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

None

Availability

None

AV:N/AC:L/Au:N/C:P/I:N/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Berkeley	Boinc Client	6.2.14	All	All	All

Application	Berkeley	Boinc Client	6.4.5	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
Trac Error – BOINC	af854a3a-2127-422b-9
BOINC "RSA_public_decrypt()" Spoofing Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com	af854a3a-2127-422b-9
oss-security - CVE Request -- tsqllib, slurm-llnl, libnasl, libcrypt-openssl-dsa-perl, erlang, boinc-client, m2crypto	af854a3a-2127-422b-9
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:003	af854a3a-2127-422b-9
#511521 - boinc: Does not check the RSA_public_decrypt() return value. - Debian Bug report logs	af854a3a-2127-422b-9
Bug 479664 – CVE-2009-0126 boinc-client: Does not check the RSA_public_decrypt() return value.	af854a3a-2127-422b-9
#823 (boinc does not check the RSA_public_decrypt() return value) - BOINC - Trac	af854a3a-2127-422b-9
Fedora update for boinc-client - Advisories - Community	af854a3a-2127-422b-9
[SECURITY] Fedora 9 Update: boinc-client-6.4.5-2.20081217svn.fc9	af854a3a-2127-422b-9
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.